enclaive

Solution Brief

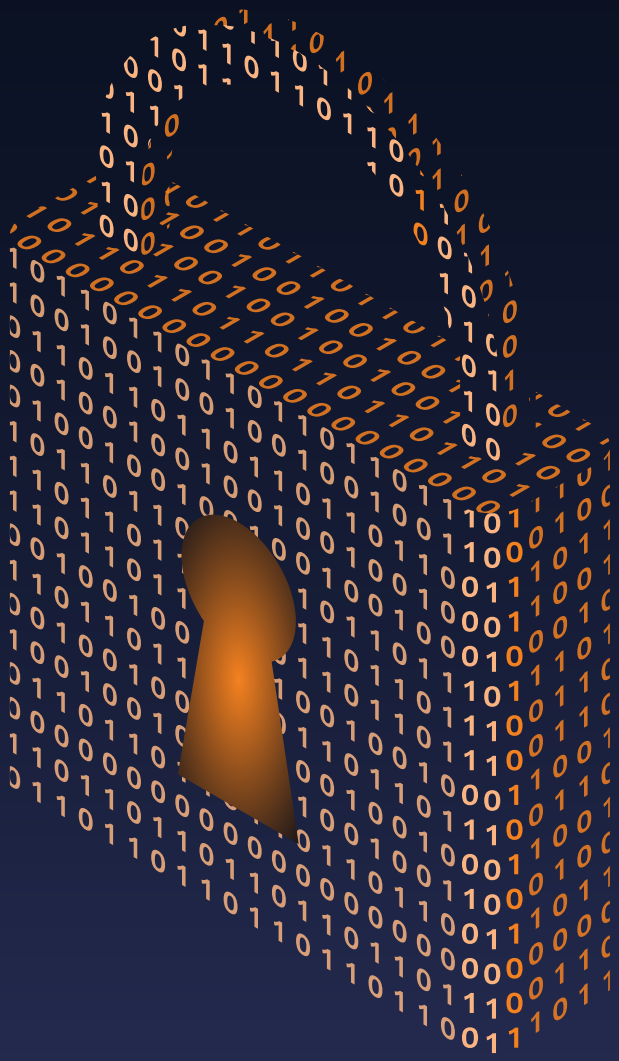
Quantum Enclaves

Der pragmatische Einstieg in Security-Architekturen für das Post-Quanten-Zeitalter

Executive Summary

Quantencomputing kommt – und es wird fundamental verändern, was wir unter digitaler Sicherheit verstehen: Verschlüsselungsverfahren, die heute als unknackbar gelten, könnten bald innerhalb von Minuten gebrochen werden. Unternehmen stehen damit vor der Herausforderung, ihre kritischen Daten, Anwendungen und Dienste schon jetzt zu schützen – bevor der sogenannte Q-Day erreicht wird.

Quantum Enclaves von enclaive helfen ihnen dabei: Als Post-Quantum-fähiges Security-Fundament ermöglichen sie es, sensible Workloads in abgeschotteten, attestierten Enklaven auszuführen, und verwenden dabei schon heute kryptographische Standards, die selbst gegenüber künftigen Quantenangriffen resilient sind. Ohne Code-Anpassungen, ohne Infrastrukturwechsel und ohne operative Komplexität.



Customer Challenge – Sicherheit mit Halbwertszeit

Quantencomputer werden die heute gängige Kryptographie aushebeln und das Ende der meisten klassischen Verfahren – von RSA und ECC bis hin zu Diffie-Hellman – einläuten. Trotz erster Initiativen, Standards und Pilotprojekten ist die Post-Quanten-Sicherheit (PQS) aber noch ein junges Thema: Laut einer Utimaco-Studie von 2025 haben erst rund 20 % der Unternehmen mit der Migration begonnen. 34 % wollen in den nächsten 1 bis 3 Jahren starten, während 25 % noch keine Pläne haben.

Im Zuge der Quantenrevolution müssen Unternehmen sich auf eine Reihe neuer Bedrohungsmodelle einstellen:

- **Kryptografie, Authentifizierung und PKI werden ausgehebelt:** Digitale Identitäten, Signaturen und Zertifikate verlieren ihre Sicherheit – mit weitreichenden Ausstrahleffekten auf Online-Banking, E-Government, Lieferketten und das gesamte Internet.
- **„Harvest now, decrypt later" wird Realität:** Viele Angreifer speichern schon seit Jahren verschlüsselte Daten, um sie in Zukunft mit Quantencomputern zu entschlüsseln. Unmengen hochkritischer Daten mit langer Lebensdauer – von Gesundheitsakten über Staatsgeheimnisse bis hin zu geistigem Eigentum – sind in Gefahr.
- **Quanten-resistente Ransomware:** Die nächste Generation der Ransomware-Angriffe könnte Post-Quanten-Kryptografie einsetzen, um die Verschlüsselung noch robuster zu machen.
- **Sabotage von Blockchains und Kryptowährungen:** Viele Kryptowährungen basieren auf elliptischer Kurvenkryptographie. Ein Quantencomputer könnte Wallets kompromittieren oder ganze Blockchains destabilisieren.

Laut einer Capgemini-Studie (2025) sehen dabei 65 % der Organisationen die „Harvest now, decrypt later"-Angriffe als besonders besorgniserregend. Knapp 60 % erwarten den sogenannten Q-Day – den Tag, an dem Kryptographie praktisch gebrochen wird – innerhalb der nächsten 10 Jahre.

Der Gesetzgeber erhöht den Druck

Auf regulatorischer Ebene hat die EU-Kommission 2024 eine Empfehlung verabschiedet, die die Mitgliedstaaten in die Pflicht nimmt, tragfähige Strategien für Post-Quantum-Kryptographie zu entwickeln. Sowohl NIS2 als auch DORA fordern zudem eine nachweisbare Absicherung kritischer Informationsinfrastrukturen. Die DSGVO verlangt bestmöglichen Schutz personenbezogener Daten. Und offizielle Stellen wie das BSI fordern proaktiv die PQ-Transformation. Unternehmen müssen das Thema also dringend auf die Agenda nehmen.

Neben dem regulatorischen wächst aber auch der technische Druck: Mehr denn je gilt es, Daten und Systeme mit langer Lebensdauer – von Geldautomaten über Medizintechnik bis hin zu Industrieanlagen – durch zukunftsfähige Kryptographie zuverlässig vor Quantenangriffen zu schützen.

Die Lösung: enclaive Quantum Enclaves

Wenn Unternehmen die ersten praktischen Schritte in Richtung PQS in Angriff nehmen, fokussieren sie sich in der Regel zunächst auf die Inventarisierung der eingesetzten kryptographischen Verfahren und die Klassifizierung besonders schützenswerter Datenbestände. Anschließend werden die ersten Pilotprojekte gestartet, die meist hybrid an das Thema herangehen und klassische Verfahren mit Post-Quanten-Kryptographie kombinieren.

Das Thema Post-Quanten-Verschlüsselung lässt sich aber auch ganz anders angehen: Zeitgemäße Ansätze im Bereich Confidential Computing schützen Daten nicht nur im Speicher (at rest) oder bei der Übertragung (in transit), sondern auch während der Verarbeitung (in use) – der Teil, den klassische Verfahren nicht schützen können. Confidential Computing verlagert sensible Workloads hierfür in hardwarebasierte, isolierte „Trusted Execution Environments“ (TEEs) – auch Enklaven genannt – und schützt Daten so in allen drei Dimensionen vor nicht-autorisierten Zugriffen.

Die Quantum Enclaves setzen sich aus folgenden Lösungen des enclaive-Portfolios zusammen:

Buckypaper

Mit Buckypaper bietet enclaive Confidential Virtual Machines (cVMs) – also VMs, die hochsicher in hardwarebasierten Enklaven ausgeführt werden. Diese Form der Virtualisierung bietet einen sicheren Weg in die Cloud, schützt vor ungewollten Zugriffen und erleichtert Lift-and-Shift-Migrationen, da die cVMs und Enklaven sich in der Regel ohne Code-Änderungen integrieren lassen – oder, falls nötig, exakt wie die bisherige On-Premises-Umgebung konfigurieren lassen.

vHSM

Das vHSM (virtual Hardware Security Module) ist enclaives innovatives, Cloud-basiertes Verschlüsselungsmodul. Es bietet skalierbare, kosteneffiziente Sicherheit für Schlüssel, Identitäten und Workloads – auf dem hohen Niveau physischer Hardware. Es ermöglicht modernes Key- und Identity-Management, erfüllt höchste Compliance-Anforderungen und integriert sich nahtlos in jede Cloud-Umgebung. Als Cloud-basierte Lösung ist es zudem stets auf dem aktuellen Stand im Hinblick auf Verschlüsselungstechnologie und regulatorische Vorgaben.

Vault

Vault ermöglicht Cloud-übergreifendes Key Management nach dem Hold-Your-Own-Key-Prinzip. Im Zusammenspiel mit dem vHSM behalten Anwender jederzeit die Kontrolle über ihre kryptografischen Schlüssel und stellen sicher, dass nur sie die Enklaven entschlüsseln können. Damit wird Vault buchstäblich zum Schlüsselfaktor digitaler Souveränität.

Nitride

Nitride stattet Workloads und Nutzer mit eindeutigen Identitäten und granularen Zugriffsrechten aus. Über kryptografische Attestation wird dabei sichergestellt, dass die Enklaven nur mit verifizierten, vertrauenswürdigen Komponenten booten. So erhalten Sie nachweisbare Integrität für vertrauliche Workloads und erfüllen mühelos Compliance- und Audit-Anforderungen.

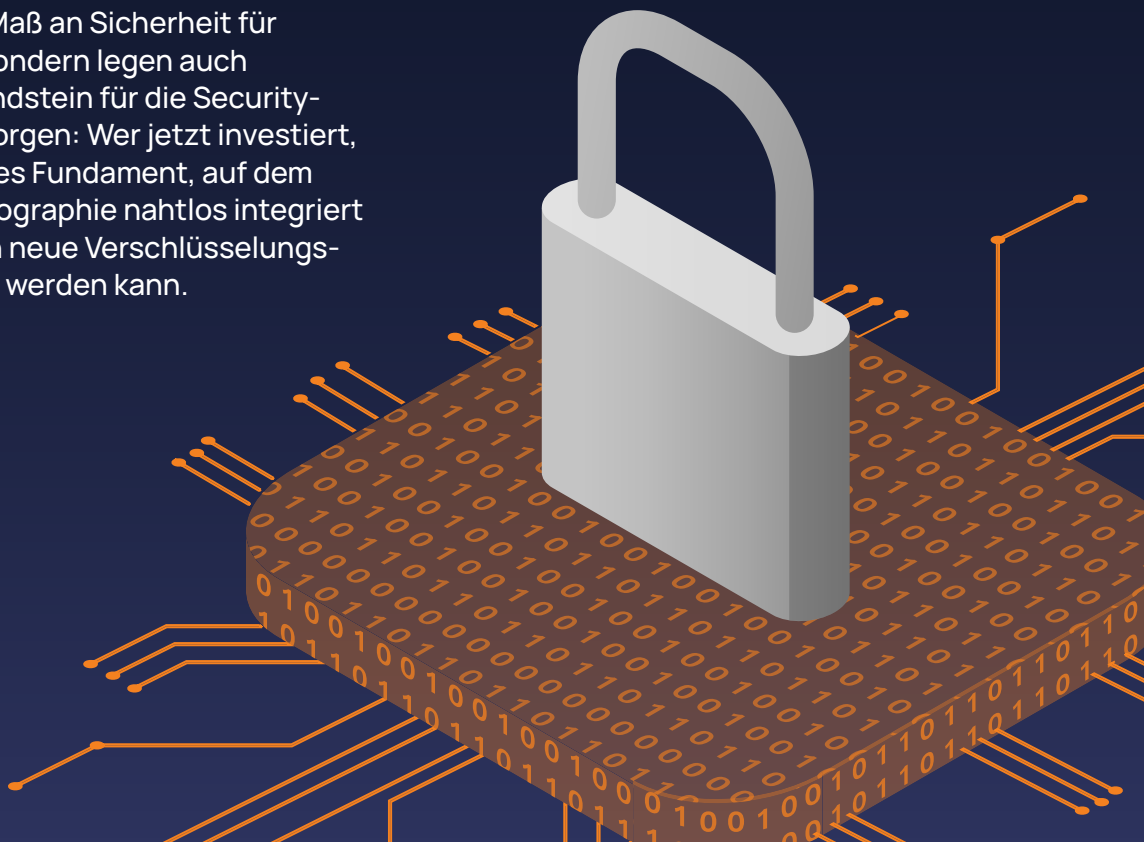
EMCP

Die eMCP (enclaive Multi-Cloud Platform) ist eine sichere, mandantenfähige Plattform, in der sich vertrauliche Datenbanken, virtuelle Maschinen und Container über verschiedene Cloud-Anbieter hinweg einrichten, betreiben und skalieren lassen. Über ein zentrales Dashboard steuern Anwender Ihre gesamte Multi-Cloud-Umgebung – von der Ressourcen- und Zugriffsverwaltung über zentrale Security- und Automatisierungseinstellungen bis hin zu Monitoring und detaillierten Analysen.

Aufsetzend auf diese Confidential-Computing-Lösungen von enclaive verwandeln die Quantum Enclaves Anwendungen – ohne jegliche Code-Modifizierung – in abgeschottete, Post-Quanten-verschlüsselte und attestierte Sicherheitszonen. Dies ermöglicht eine sichere Datenverarbeitung in der Cloud und verhindert zuverlässig, dass Secrets jemals im Klartext sichtbar werden – weder für Administratoren, noch für Angreifer, noch für kompromittierte Betriebssysteme oder neugierige Cloud-Provider.

Mit Quantum Enclaves stellen Unternehmen also schon jetzt die Weichen für weitreichende digitale Souveränität und behalten jederzeit die Kontrolle über ihre Schlüssel und Daten. Gerade mit Blick auf mögliche Aktivitäten staatlicher Akteure mit leistungsstarker Quantentechnologie ein wichtiger Vorteil.

Auf diese Weise sichern sich Unternehmen nicht nur ein hohes Maß an Sicherheit für das Hier und Jetzt, sondern legen auch einen wichtigen Grundstein für die Security-Architekturen von Morgen: Wer jetzt investiert, schafft ein tragfähiges Fundament, auf dem Post-Quanten-Kryptographie nahtlos integriert und kontinuierlich an neue Verschlüsselungsverfahren angepasst werden kann.



Key Benefits – Sicherheit, die auch morgen noch schützt

Quantum Enclaves von enclaive bieten Unternehmen in dreifacher Hinsicht entscheidende Vorteile:

Zukunftssichere Security-Architektur
Mit den Quantum Enclaves profitieren Unternehmen von einer hochsicheren Umgebung, in der sie Anwendungen und Daten zuverlässig schützen und betreiben können – sowohl heute als auch in der Post-Quanten-Ära. So gibt die Lösung eine pragmatische und operative Antwort auf die Unsicherheit des Zeitpunkts, an dem klassische Kryptographie versagt.

Weichenstellung für Compliance & Governance
Auditierbare Attestation und garantierte Isolation ermöglichen es Unternehmen, regulatorische Anforderungen nicht nur zu erfüllen, sondern auch zweifelsfrei gegenüber Prüfern nachzuweisen – inklusive Daten-Souveränität, Cloud-Unabhängigkeit und kontrollierbaren Security-Domains.

Quantum-Readiness als Wachstumstreiber
Das Plus an Sicherheit bietet auch wirtschaftlich handfeste Vorzüge– von geringeren Haftungsrisiken über niedrigere Kosten im Incident-Handling bis hin zu verkürzten Audit-Zyklen und dem zuverlässigen Schutz geschäftskritischer Geheimnisse. Unternehmen werden so in die Lage versetzt, ihre Sicherheitsstrategie nicht nur zu verteidigen, sondern aktiv als Innovationstreiber einzusetzen.

Use Cases

Der Einsatz von Quantum Enclaves empfiehlt sich im ersten Schritt besonders bei Workloads mit hoher Risikointensität, zum Beispiel:

- **Finanz- und Zahlungsverkehr:** Im Finanzsektor treffen strenge Compliance-Vorgaben – zunehmend auch zur Post-Quanten-Kryptografie – auf vertrauliche Daten wie Kredit- und Wertpapierunterlagen, Transaktionshistorien und Risikoanalysen. Quantum Enclaves schützen diese langlebigen Finanzdaten, gewährleisten den sicheren Austausch von Informationen über Institutionsgrenzen hinweg und schaffen so eine vertrauenswürdige Basis für digitale Vermögenswerte und Zahlungsinfrastrukturen.
- **Staatliche und kritische Infrastrukturen:** Behördliche Register, VS-NfD-Informationen oder KRITIS-Systeme haben immense Schutz- und Langzeitrelevanz. Post-Quanten-Enklaven sichern diese gegen heutige wie künftige Entschlüsselungsangriffe, schützen Verwaltungsprozesse und gewährleisten die Verfügbarkeit digitaler Dienste. Sie stärken sowohl Innere als auch Nationale Sicherheit, indem sie staatliche und militärische Netzwerke, Behörden-Operationen und kritische Versorgungsinfrastrukturen langfristig resilient gegen Spionage und Manipulation machen.

- **Gesundheitswesen:** Gesundheitsdaten sind hochsensibel und oft lebenslang relevant. Quantum Enclaves schützen diese Daten zukunftssicher – und gewährleisten einen Informationsaustausch in sicheren Datenräumen zwischen Organisationen, Institutionen und Behörden. Das verbessert Versorgung, Forschung und gesundheitspolitische Entscheidungen und erfüllt zugleich die hohen regulatorischen Anforderungen der DSGVO sowie von BSI und gematik.

- **Industrial IoT:** Im industriellen Umfeld schützen Post-Quanten-Enklaven vernetzte Geräte, Maschinenkonfigurationen und Produktionsgeheimnisse zuverlässig in jeder Umgebung, auch in fremden Rechenzentren. Weder kompromittierte Hosts noch Side-Channel-Angriffe oder unbefugte Provider-Zugriffe gefährden die Integrität oder Vertraulichkeit der Daten. Confidential Computing verhindert effektiv Cyber-Sabotage und ermöglicht Unternehmen eine robuste Mikrosegmentierung, manipulationsfreie Fernwartung und geschützte digitale Zwillinge.

- **KI & Machine Learning:** KI-Modelle und Trainingsdaten zählen zum wertvollsten geistigen Eigentum vieler Unternehmen. Quantum Enclaves schützen Modellartefakte, Feature-Stores und ganze Inference-Pipelines zuverlässig vor Datendiebstahl. Sie ermöglichen zudem vertrauliches Training (Federated Learning, Secure Aggregation) und die sichere Interaktion mit internen Modellen. Ergänzend bietet enclaive mit Garnet eine GenAI-Firewall, die sensible Informationen vor der Interaktion mit externen KI-Modellen innerhalb der Enklave filtert und pseudonymisiert.

Fazit

Quantum Enclaves kapseln Anwendungen in einer gehärteten Ausführungsumgebung, die kryptographisch attestiert und vollständig verschlüsselt ist. Die Prozesse laufen darin wie in einem digitalen Tresor, der selbst dem Betreiber verborgen bleibt.

Aufsetzend auf standardisierte Schnittstellen lässt sich eine solche Lösung nahtlos in Kubernetes-Cluster, Multi-Cloud-Deployments oder On-Prem-Architekturen integrieren. Unternehmen behalten dabei volle Souveränität über Schlüssel und Standortkontrolle – selbst dann, wenn sie Public-Cloud-Ressourcen einsetzen.

enclaive fungiert damit auch als Brücke: von heutigen Infrastrukturen hin zu einer vollständig Post-Quantum-sicheren IT-Landschaft. Bereits genutzter Schutz bleibt erhalten und wächst mit zukünftigen Standards weiter.

Starten Sie mit uns jetzt ins Post-Quanten-Zeitalter!

Die Migration in die Post-Quanten-Ära ist kein Sprint, sondern eine Transformation. Aber sie beginnt mit einem einzigen, entscheidenden Schritt: Die wichtigsten Daten zuerst schützen.

enclaive bietet dazu einen schnellen und risikoarmen Einstieg:

- Gemeinsamer Quantum-Readiness-Workshop
- Identifikation der kritischen Workloads
- PoC-Deployment ausgewählter Anwendungen in Quantum Enclaves
- Compliance-Mapping und operative Integration in DevSecOps-Prozesse

Wenn Sie mit uns heute auf diesem Weg starten, profitieren Sie doppelt: Sie gewinnen sofort mehr Sicherheit — und legen ein tragfähiges Fundament, das auch in der Post-Quanten-Zukunft Bestand hat.

Kontakt: sales@enclaive.io
Mehr Informationen: enclaive.io